Kaspersky®
Secure Hypervisor

Kaspersky Lab Cybersecurity for SCADA & ICS

SCADA as a complex system

Industrial control systems are highly complex and need to meet a wide range of requirements. ICSs have to perform a huge number of functions, have high availability, include safety indicators, support multiple sites, operate within hard real-time constraints and conform to legislation.

A modern ICS is a mixture of technologies, standards and protocols including those from outdated and legacy systems. We should also mention that ICSs often include embedded components with resource constraints.

Cybersecurity requirements are often underestimated.

Common misconceptions include:

Misconceptions	In reality
ICSs use proprietary standards and protocols that only experts know about and this information is not available to hackers.	ICS documentation, protocol specifications, etc. are available on the internet, including descriptions of vulnerabilities and 'how to hack' manuals.
ICSs operate in a closed environment.	Many ICS networks are directly or indirectly connected to public networks and ICS services can become a target for remote attackers.
ICSs cannot be attacked from within an organization.	Many people work with ICS systems. It's impossible to guarantee there is no internal attacker among them. Confused deputy problems are also an issue.
It's possible to avoid risks by using up-to-date technologies.	An ICS lifetime is very long and it's difficult to keep it in an up-to-date state. During this time technologies may become obsolete.

Cybersecurity aspects
Management
Technology
Human factor
Operational maintenance
External and internal environment

IT security requirements	ICS security requirements
Confidentiality Integrity Availability	Availability Integrity Confidentiality Safety Environment Dependencies Regulation Others

Examples of attacks
Buffer overflow attack
Code injection attack
Input validation issue attack
Physical access-based attacks
Credentials attack
Lack of authentication attack
Weak implementation of cryptography
Path traversal attack
Web browsing attack
Cross-site request forgery
Resource exhaustion attack

Sources of threats and issues

Cybersecurity requires a holistic approach, with a security analysis that addresses the following aspects:

1. **Management:**
   - Cybersecurity is not considered a core business objective;
   - ICSs are not considered part of the IT infrastructure;
   - Lack of education and training;
   - Depreciation (cybersecurity aspect) and procurement.

2. **Technology:**
   - Legacy technologies;
   - Insecurity by design;
   - Protocols that are insecure or not attack-resilient;
   - Wrong operational environment assumptions;
   - Remote access.

3. **Human factor:**
   - Lack of policies and procedures;
   - Potential attacks from system residents and from ex-employees;
   - Confused deputy problem.

4. **Operational maintenance:**
   - Credentials management problem;
   - Lack of change management procedures and consequence analysis;
   - Superuser administrator problem;
   - Patching problems;
   - Malware protection;
   - Access to hardware and networks.

5. **External and internal environment:**
   - Physical security;
   - Dependencies (power supply, IT infrastructure);
   - Third-party and remote access.

For certain groups of cybercriminals ICSs are a high-level target. There are a number of reasons for this, but we'll mention just two of them here. The first is that the attacked object can sustain potentially catastrophic damage that could impact individuals, organizations, the environment and even society at large. The second reason is that the attack surface is extremely large – an ICS consists of many technologies, and many of them are unsecure.

The goals of an attack can vary. For example, it might be to sabotage an industrial system for financial gain in the form of a ransom, to gain a competitive advantage, to carry out a terrorist attack, or even as a simple act of cybervandalism.

These attacks are made possible due to vulnerabilities such as design flaws, implementation flaws, backdoors and improper usage of the system.

Kaspersky Lab offers technologies capable of significantly improving the security of industrial cybersystems.

Kaspersky Secure Hypervisor for SCADA cybersecurity

As well as a long list of traditional cybersecurity products for enterprises and home users, Kaspersky Lab has several specialized products: KasperskyOS, Kaspersky Security System (KSS) and Kaspersky Secure Hypervisor (KSH). The key feature of all three is an innovative approach that makes it possible to thoroughly control inter-process communications in accordance with specified security policies.

Kaspersky Secure Hypervisor is a Type 2 hypervisor that runs on top of the KasperskyOS microkernel. The main benefit of a virtualization solution is the separation of potentially untrusted guest operating systems from each other and from critical services collocated on the same physical machine, reducing the attack surface and minimizing the possible impact of exploited vulnerabilities. The hypervisor is protected from guest OS actions in such a way that malicious activities by a guest system cannot damage the critical services or the hypervisor itself. An additional benefit of KSH is its ability to reduce expenses on hardware maintenance.

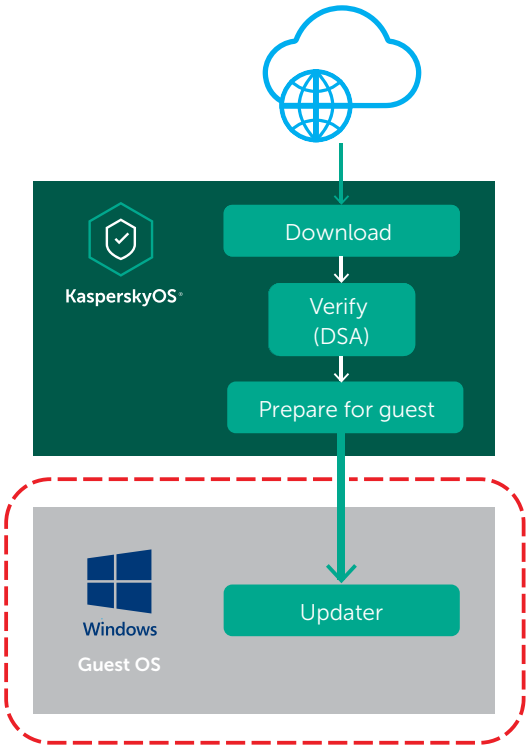
We recommend using KSH to ensure the cybersecurity of SCADA systems. The use of a special hypervisor-based solution makes it possible to solve a range of SCADA cybersecurity issues with no modification or upgrade of SCADA software.

We propose several protection scenarios that can be implemented with the help of KSH.

1. Control for peripherals

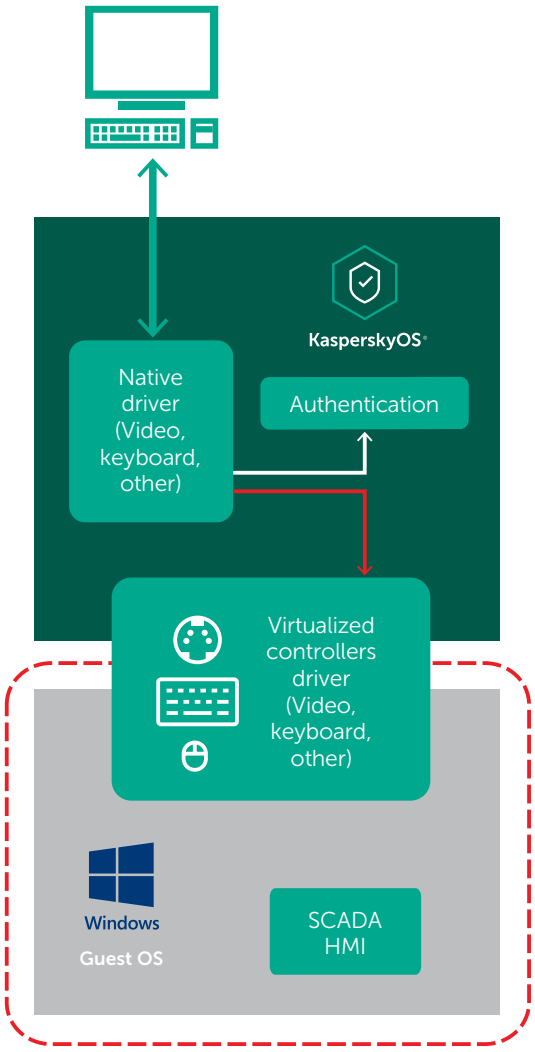
As KSH ensures complete isolation for guest operating systems, it can grant or refuse access to peripherals. For example, KSH can:

- Disable unused peripherals (USB, Bluetooth, Wi-Fi, camera, microphone) and reduce the attack surface.
- Control access to peripherals in accordance with a security policy (in conjunction with KSS).
- Authorize user access to peripherals.



2. Secure update

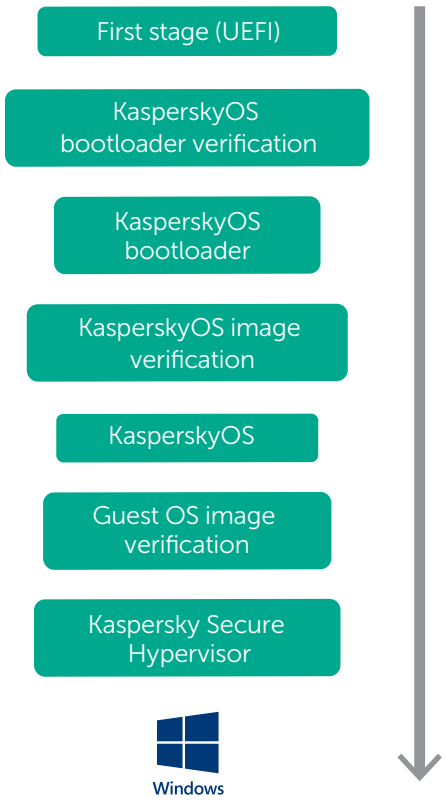
According to statistics, some malicious programs are loaded to systems during the update process. Secure update with KSH is a reliable way to keep SCADA and its components in an up-to-date and secure state. KSH provides an independent channel for update delivery. It helps control the process, verifying the integrity and authenticity of the update. Even if an update image is downloaded from an untrusted source, it will be verified by secure mechanisms.



3. Trusted authentication

Because guest OSs are complex systems and can include many vulnerabilities and problems, we can't trust their native authentication mechanisms. KSH operates in a trusted environment, so can provide additional independent and reliable authentication on the KasperskyOS level.

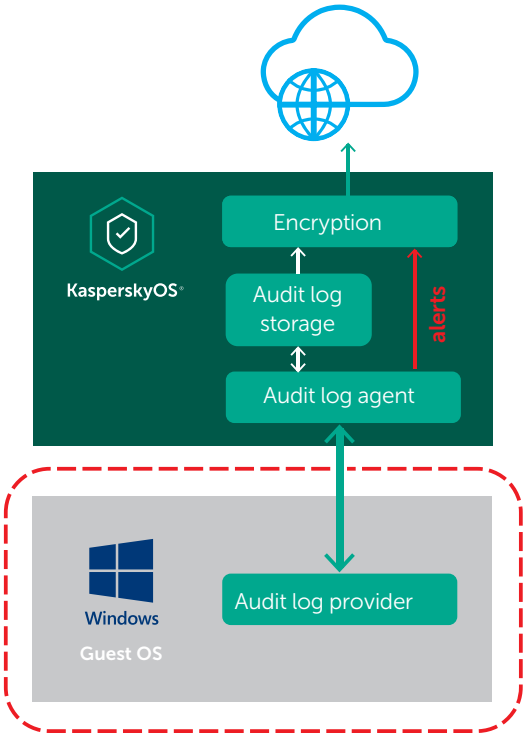
When trying to access a guest OS a user has to pass KSH authorization. The KSH authentication application interacts with the hardware. After successful authentication the hypervisor provides the SCADA HMI access to the hardware from the guest OS via virtualized controller. In addition, with KSH it's possible to provide a variety of authentication schemes that are not supported by guest OSs (password, token, smart card, fingerprint, etc.).



4. Secure boot

KSH makes it possible to provide a secure boot of a guest OS, a basic security measure for embedded systems. Secure boot implementation involves a set of verification procedures based on hardware protection mechanisms.

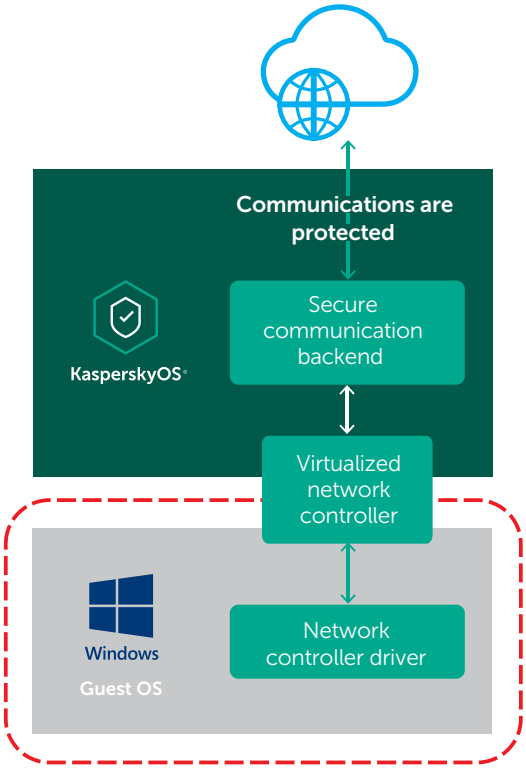
A secure boot ensures the integrity and authenticity of an OS image (OS core and file systems) and its loaders, and guarantees that an operating system damaged or modified by an attacker is not booted.



5. Secure audit log

With KSH it's possible to prevent audit log spoofing in a guest OS. A trusted channel between KSH and the guest OS makes it possible to deliver the audit log that's securely stored in KSH (there's a range of options for protecting the log – from storing it as a file on the KSH side to a blockchain-based approach that guarantees spoofing protection even if a device is physically accessed).

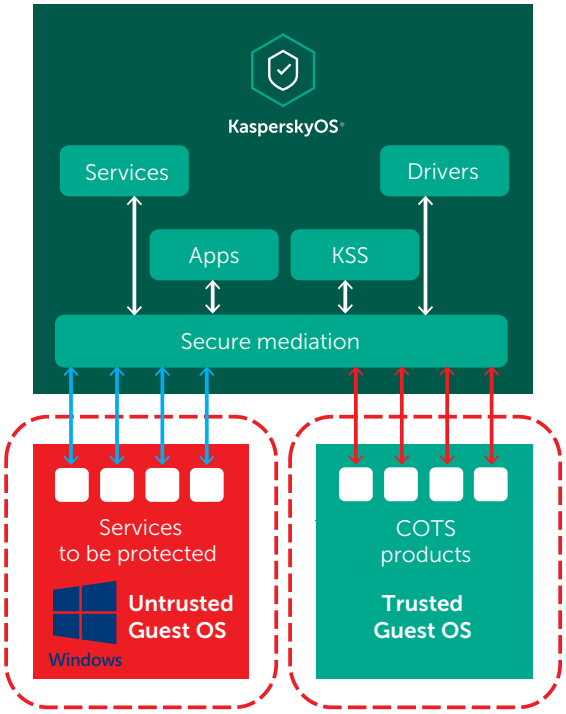
Additional state-of-the-art encryption can be performed with KSH that helps integrate log storage and delivery to the customer's current or new infrastructure.



6. Protection for distributed systems

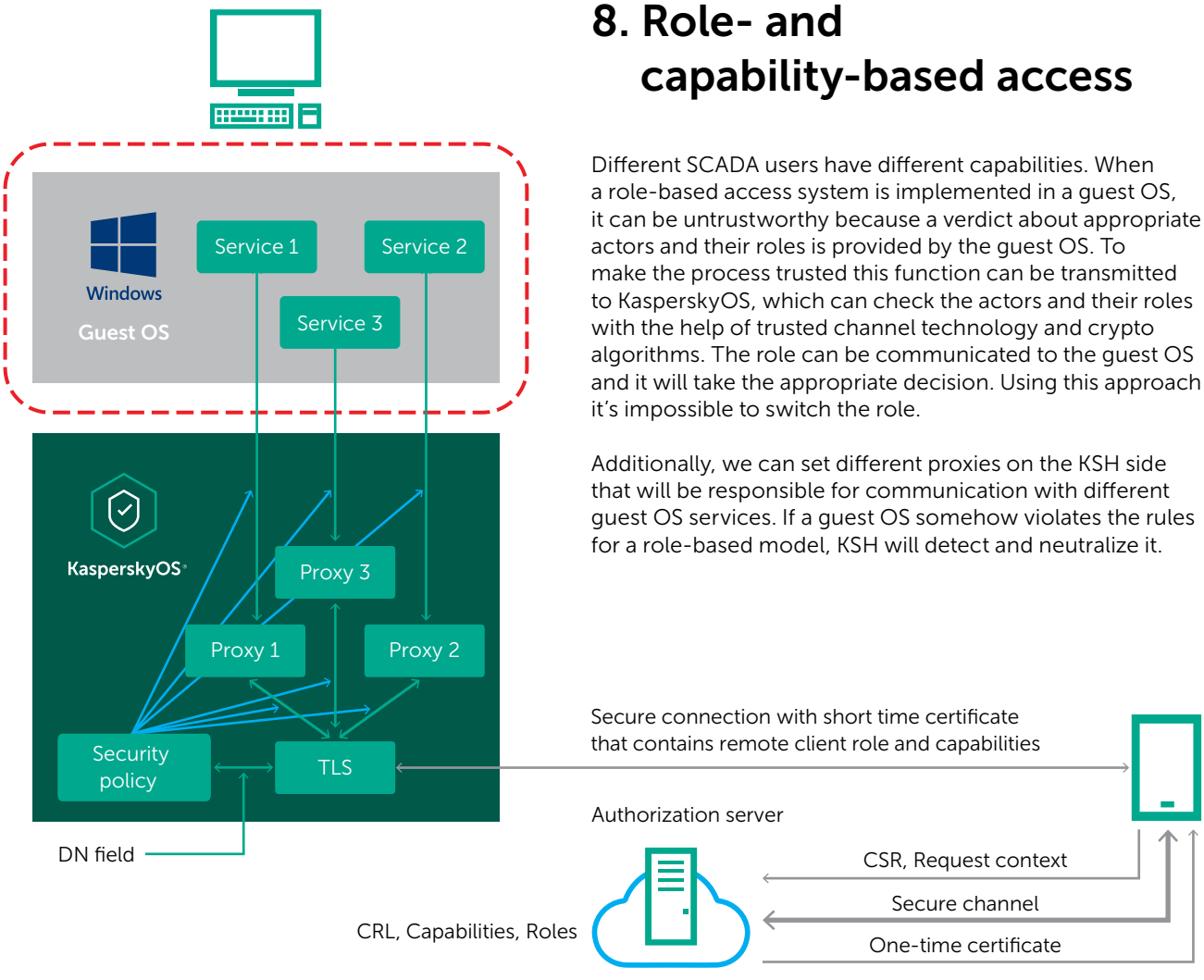
Distributed SCADA systems can be very complex and have a heterogeneous structure. They are often hard to support because there's no single administration point. They contain security holes that are extremely hard to detect or a mixture of obsolete protocols that may have vulnerabilities (e.g. SSL v3.0). Upgrading such systems can be difficult and expensive. In many cases, system owners choose system availability over security, so these systems become vulnerable.

KSH provides a trusted channel protected with the best encryption technologies. A guest OS views this channel as a simple network adaptor, so it continues to send data with no additional measures. KSH receives an unprotected packet, encrypts it and organizes a protected private network. This helps prevent data spoofing or leakage.



7. Secure solution with additional trusted guest

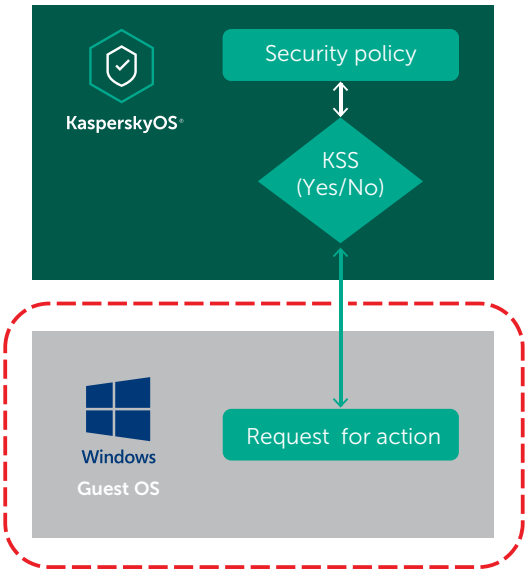
If the extra work required to adopt existing technologies and products to attain a completely secure infrastructure seems like too much effort, with KSH it's possible to install a small trusted guest OS that can even be Linux-based (of course, certain additional restrictive measures are required). A set of ready applications that don't need any additional development can be installed on this trusted guest OS. These applications can include different cryptographic protocols, DPIs and administration tools. KSH ensures secure communication between the trusted OS and an untrusted OS.



8. Role- and capability-based access

Different SCADA users have different capabilities. When a role-based access system is implemented in a guest OS, it can be untrustworthy because a verdict about appropriate actors and their roles is provided by the guest OS. To make the process trusted this function can be transmitted to KasperskyOS, which can check the actors and their roles with the help of trusted channel technology and crypto algorithms. The role can be communicated to the guest OS and it will take the appropriate decision. Using this approach it's impossible to switch the role.

Additionally, we can set different proxies on the KSH side that will be responsible for communication with different guest OS services. If a guest OS somehow violates the rules for a role-based model, KSH will detect and neutralize it.



9. Authorization of guest actions

KSH provides a toolset to manage guest OS software behavior in accordance with the security policies defined for the overall solution. In the majority of practically important use cases, the guest OS can be considered trusted to run ICS applications, but the actions performed by applications may require additional control. Due to possible bugs, design flaws or erroneous user actions, ICS applications may perform dangerous or prohibited operations. To avoid these situations KSH provides an interface that allows the guest OS applications to request additional authorization for its operations. Using this interface, the guest OS software can directly address Kaspersky Security System. Then KSS, using the security policy that's defined for the solution as a whole, computes a verdict, whether the operation is possible or not, and reports back. In the event of a negative verdict, the guest OS software can block the operation. In other words, the guest OS software uses an independent mechanism that helps match its operations with the solution's overall security policy.

10. Other

Other protection technologies can be supplied with KSH.

Trusted Execution Environment (TEE) for Guest OS is one of them. Certain functions (cryptography or storage) can be placed outside the guest OS –
in a secure environment on the level of KSH.

The unique protection services of KSH mean we can restrict access by guest OSs to any resources (for example, memory or periphery).

KSH can also ensure guest OS health monitoring: memory usage, watchdog functionality, high load alert, resource exhaustion alert.

There is also a set of supplementary services that can be implemented. For example, any security policies can be implemented for a guest OS, trusted platform management, backup and restore service and many others.

PcVue Secure

powerful SCADA/HMI hardened
with Kaspersky Secure Hypervisor

Current projects

Kaspersky Secure Hypervisor is a new product on the market. Kaspersky Lab is currently working on a new project together with ARC Informatique, a leading European developer and manufacturer of software for industrial systems. Within the scope of the project we plan to create a new product for SCADA based on the technologies of PcVue and KSH. This joint product will take SCADA cybersecurity to a new level, giving customers greater confidence that their industrial control systems will operate securely and stably.

www.kaspersky.com

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

Kaspersky Lab's threat researches and reports: www.securelist.com

KasperskyOS®: os.kaspersky.com

#kasperskyos
#truecybersecurity